



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/733,469	12/12/2003	Victor J. Yodaiken	0125-143	8829
6449	7590	12/14/2007		
ROTHWELL, FIGG, ERNST & MANBECK, P.C. 1425 K STREET, N.W. SUITE 800 WASHINGTON, DC 20005			EXAMINER DEBNATH, SUMAN	
			ART UNIT 2135	PAPER NUMBER
			NOTIFICATION DATE 12/14/2007	DELIVERY MODE ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO-PAT-Email@rfem.com

AW

<b>Office Action Summary</b>	Application No. 10/733,469	Applicant(s) YODAIKEN, VICTOR J.	
	Examiner Suman Debnath	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 13 September 2007.  
 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.  
 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-7, 14-20 and 25-44 is/are pending in the application.  
     4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
 6) ☒ Claim(s) 1-7, 14-20 and 25-44 is/are rejected.  
 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.  
 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
     a) ☐ All    b) ☐ Some \*    c) ☐ None of:  
         1. ☐ Certified copies of the priority documents have been received.  
         2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
         3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
     \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

1. Claims 1-7, 14-20 and 25-44 are pending in this application.
2. Claims 1-2, 4-7, 14-17 and 25-26 are presently amended.
3. Claims 8-13 and 21-24 are cancelled.
4. Claims 39-44 have been newly presented in the amendment filed 13 September 2007.
5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office Action.

***Claim Objections***

6. Claim 1 is objected to because of the following informalities:  
  
It recites "the computer system" in line 11, 12 and 21.  
  
Appropriate correction and/or clarification is required.

***Claim Rejections - 35 USC § 112***

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:  
  
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
8. Claims 1, 2, 39 and 42 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

9. Regarding claims 1 and 2, the limitation "**about** five millisecond" in line 16 of claim 1 and in line 13 of claim 2 renders the claims indefinite because it is unclear whether a response should take more than five millisecond or exactly five millisecond or less than five millisecond. The phrase "about" makes it impossible to determine if there is any upper or lower boundary of time taken for a response.

10. Claims 39 and 72 are rejected for the same reason as claims 1 and 2.

***Claim Rejections - 35 USC § 103***

11. Claims 1-2, 39-40 and 42-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Douglas (Patent No.: US 7,152,242 B2) and further in view of O'Neal et al. (Patent No.: US 6,640,242 B1), hereinafter "O'Neal".

12. As to claim 1, Douglas discloses a computer system, comprising:

a computer executing a hard real-time operating system, said computer being connected to the network (abstract, col. 2, lines 30-50);

an application running under the hard real-time operating system (col. 2, lines 30-50);-and

a security process running under the hard real-time operating system (col. 9, lines 3-15); and

an external monitor connected to the network (col. 2, lines 30-50), wherein the security process is configured to periodically, in hard real-time, check the integrity of the

application and/or a data element used by the application (col. 9, lines 3-15) and, if the integrity check of the application or the data element indicates that the application or data element has been tampered with, notify a user of the computer system and/or shut down at least part of the computer system or application (col. 2, lines 45-60), and

Douglas doesn't explicitly disclose a deterministic network; the security process includes a challenge handler that is configured to (i) receive a challenge transmitted from -the external monitor to the challenge handler via the deterministic network and (ii) transmit to the external monitor via the deterministic network a response to the challenge in less than about five millisecond from the challenge handler receiving the challenge wherein the external monitor is configured so that if the external monitor does not receive the response within five milliseconds or less from sending the challenge, the external monitor issues a notification notifies an and/or shuts down at least part of the computer system or application.

However, O'Neal discloses a deterministic network (O'Neal teaches deterministic network by setting a predetermined time on response messages; responds are sent within a predetermined amount of time which makes the network to be deterministic, - e.g. see -col. 19, lines 10-20); the security process includes a challenge handler that is configured to (i) receive a challenge transmitted from -the external monitor to the challenge handler via the deterministic network and (ii) transmit to the external monitor via the deterministic network a response to the challenge in less than about five millisecond from the challenge handler receiving the challenge wherein the external monitor is configured so that if the external monitor does not receive the response within

five milliseconds or less from sending the challenge (col. 9, lines 10-25, Applicant should note that the phrase "about" makes it indefinite to set an upper or lower boundary to how long a response should take. O'Neal discloses response takes predetermined amount of time. Applicant should note that "a predetermined amount of time" can be configured as any give time), the external monitor issues a notification notifies an and/or shuts down at least part of the computer system or application (col. 9, lines 10-25, "If a system or sub-system fails to respond within a predetermined amount of time, monitor 216 alerts a system...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Douglas as taught by O'Neal in order to protect resources and to ensure safe and secure operations.

13. As to claim 2, Douglas discloses in a computer system running a real-time operating system, a computer security method (abstract), comprising:

executing a security process under the real-time operating system (col. 9, lines 3-15), wherein the security process is configured to periodically, in hard real-time, check the integrity of an application and/or a data element used by the application (col. 9, lines 3-15, "The HIDS sensor 20 is capable of monitoring the integrity of the Linux kernel", see also col. 4, lines 44-60) and issue a notification and/or shut down the application if the integrity check of the application or the data element indicates that the application or data element has been tampered with (col. 2, lines 45-60);

Douglas doesn't explicitly disclose sending from an external monitor, a challenge to the security process or to a challenge handler that monitors the integrity of the security process via a deterministic network; sending to the external monitor via the deterministic network a response to the challenge, wherein the response is sent in less than about five milliseconds from when the challenge was received; and issuing a notification and/or shutting down at least part of the computer system or the application notifying if a response to the challenge is not received within about five milliseconds or less from when the challenge was sent.

However, O'Neal discloses sending from an external monitor, a challenge to the security process or to a challenge handler that monitors the integrity of the security process via a deterministic network (O'Neal teaches deterministic network by setting a predetermined time on response messages; responds are sent within a predetermined amount of time which makes the network to be deterministic, - e.g. see -col. 19, lines 10-20); sending to the external monitor via the deterministic network a response to the challenge, wherein the response is sent in less than about five milliseconds from when the challenge was received (col. 9, lines 10-25, Applicant should note that the phrase "about" makes it indefinite to set an upper or lower boundary to how long a response should take. O'Neal discloses response takes predetermined amount of time. Applicant should note that "a predetermined amount of time" can be configured as any give time); and issuing a notification and/or shutting down at least part of the computer system or the application notifying if a response to the challenge is not received within about five milliseconds or less from when the challenge was sent (col. 9, lines 10-25, "If a system

or sub-system fails to respond within a predetermined amount of time, monitor 216 alerts a system...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Douglas as taught by O'Neal in order to protect resources and to ensure safe and secure operations.

14. As to claims 39 and 42, Douglas doesn't explicitly disclose wherein the challenge handler is configured to provide a response within about one millisecond. However, O'Neal discloses wherein the challenge handler is configured to provide a response within about one millisecond (col. 9, lines 10-25).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Douglas as taught by O'Neal in order to in order to protect resources and to ensure safe and secure operations.

15. As to claims 40 and 43, Douglas discloses wherein the security process is configured at system boot with a periodicity to check the integrity of the application (column 9, lines 3-15).

16. Claims 3, 27 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over REDSonic, Inc, "<http://www.redsonic.com/en/products/RealTime.htm>"; Copyright 2002, pp 1-4, hereinafter "Sonic" and further in view of Douglas.



17. Claims 3, 27 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over REDSonic, Inc, "<http://www.redsonic.com/en/products/RealTime.htm>"; Copyright 2002, pp 1-4, hereinafter "Sonic" and further in view of Douglas.

18. As to claim 3, Sonic discloses a computer system, comprising: a dual-kernel operating system comprising a real-time kernel (page 1, Sonic teaches this concept by disclosing the real-time kernel which inserts a thin layer between the interrupt-control hardware and the standard Linux kernel) and a non-real-time kernel ("Linux Kernel" – e.g. page 1); a first real-time thread running under the real-time kernel (page 1, Sonic teaches this concept by disclosing "real-time Linux kernel as a small real-time OS that can suspend Linux's execution at any state"), the first real-time thread being configured to monitor an application running under the non-real-time kernel (page 1, Sonic teaches this concept by disclosing the real-time kernel which inserts a thin layer between the interrupt-control hardware and the standard Linux kernel);

Sonic doesn't explicitly disclose the first thread being configured to monitor the integrity of an application; a second real-time thread running under the real-time kernel, the second real-time thread being configured to monitor integrity of the first real-time thread; and a security process running under the non-real-time kernel, the security process being configured to-check the integrity of the first real-time thread and/or the second real-time thread.

However, Douglas discloses the first thread being configured to monitor the integrity of an application (col. 2, lines 45-50, "...integrity checking feature"); a second

real-time thread running under the real-time kernel (col. 2, lines 35-60, which describes file integrity checking feature for an additional level of detection. Applicant should note that Douglas has integrity checking feature which would require real time processing in order to maintain the integrity of applications), the second real-time thread being configured to monitor integrity of the first real-time thread (col. 2, lines 35-60); and a security process running under the non-real-time kernel, the security process being configured to check the integrity of the first real-time thread and/or the second real-time thread (column 9, lines 3-15, "The HIDS sensor 20 is capable of monitoring the integrity of the Linux kernel", see also column 4, lines 44-60, in which sensor reads as security process which being configured to check the integrity of threads that are running under Linux kernel).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Sonic as taught by Douglas in order to provide notification of the intrusion or intrusion attempts.

19. As to claim 27, Sonic doesn't explicitly disclose wherein the first real-time thread is further configured to check a set of integrity markers of the non-real-time kernel. However, Douglas discloses wherein the first real-time thread is further configured to check a set of integrity markers of the non-real-time kernel (column 2, lines 45-50, "...integrity checking feature").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Sonic as taught by Douglas in order to "provide notification of the intrusion or intrusion attempts."

20. As to claim 31, Sonic doesn't explicitly disclose wherein the second real-time thread is further configured to check a set of integrity markers of the real-time kernel. However, Douglas discloses wherein the second real-time thread is further configured to check a set of integrity markers of the real-time kernel (column 2, lines 45-50).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Sonic as taught by Douglas in order to "provide notification of the intrusion or intrusion attempts."

21. Claims 4-5 and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Douglas and further in view of O'Neal and Williams et al. (Patent No.: 5,911,065), hereinafter "Williams".

22. As to claims 4 and 17, neither Douglas nor O'Neal explicitly discloses wherein the integrity check performed by the security process includes checking an execution schedule of the application. However, Williams discloses wherein the integrity check performed by the security process includes checking an execution schedule of the application (abstract, column 4, lines 39-45 and column 6, lines 30-40).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Douglas and O'Neal as taught by Williams in order to ensuring that the time sequence for the delivery of interrupts is not altered.

23. As to claims 5 and 18, neither Douglas nor O'Neal explicitly discloses wherein the security process is configured to raise an alarm if, after checking the execution schedule of the application, the security process determines that the application is not being scheduled at a required minimum frequency. However, Williams discloses wherein the security process is configured to raise an alarm if, after checking the execution schedule of the application, the security process determines that the application is not being scheduled at a required minimum frequency (abstract, column 4, lines 39-45 and column 6, lines 30-40).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Douglas and O'Neal as taught by Williams in order to ensuring that the time sequence for the delivery of interrupts is not altered.

24. Claims 6-7, 14 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Douglas and further in view of O'Neal and Terry (Pub. No.: US 2002/0026505 A1).

25. As to claims 6 and 19, neither Douglas nor O'Neal explicitly discloses wherein the integrity check performed by the security process includes checking the integrity of the application's code. However, Terry discloses wherein the integrity check performed by the security process includes checking the integrity of the application's code ([0074]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Douglas and O'Neal as taught by Terry in order to report any modifications to management personnel within a business or organization.

26. As to claims 7 and 20, neither Douglas nor O'Neal discloses wherein the security process is configured to raise an alarm if, after checking the integrity of the application's code, the security process determines that the application code has been tampered with. However, Terry discloses wherein the security process is configured to raise an alarm if, after checking the integrity of the application's code, the security process determines that the application code has been tampered with ([0074], "...reports (alerts) the administrative application").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Douglas and O'Neal as taught by Terry in order to report any modifications to management personnel within a business or organization.

27. As to claim 14, neither Douglas nor O'Neal explicitly discloses wherein the security process is further configured to update a data item with a sequence number indicating a number of cycles that have passed without detection of an intruder.

However, Terry discloses wherein the security process is further configured to update a data item with a sequence number indicating a number of cycles that have passed without detection of an intruder ([0058] – [0059]).

Therefore, it would have been obvious to one of ordinary skill in the art the time of the invention was made to modify the teaching of Douglas and O'Neal as taught by Terry in order to report any modifications to management personnel within a business or organization.

28. Claims 25-26, 41 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Douglas and further in view of O'Neal and Berg et al. (Pub. No.: US 2001/0044904 A1), hereinafter "Berg".

29. As to claim 25, neither Douglas nor O'Neal explicitly disclose further comprising sending an encryption key to the security process at or about the same time as sending the challenge to the security process. However, Berg discloses sending an encryption key to the security process at or about the same time as sending the challenge to the security process ([0071]-[0072]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Douglas and O'Neal as taught by Berg in order to ensure the confidentiality of sensitive information.

30. As to claim 26, neither Douglas nor O'Neal explicitly discloses further comprising receiving the encryption key and encrypting the response using the encryption key prior to transmitting the response. However, Berg discloses further comprising receiving the encryption key and encrypting the response using the encryption key prior to transmitting the response ([0007], [0027], lines 16-24 and [0072]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Douglas and O'Neal as taught by Berg in order to ensure the confidentiality of sensitive information.

31. As to claims 41 and 44, neither Douglas nor O'Neal explicitly discloses wherein the response is encrypted. However, Berg discloses wherein the response is encrypted ([0007], which describes encrypting and decrypting communications).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Douglas and O'Neal as taught by Berg in order to increase the security of transferred data.

32. Claims 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sonic and further in view of Douglas and Berg.

33. As to claim 28, neither Sonic nor Douglas explicitly discloses wherein the integrity markers include a checksum and/or digital signature of a data element that maintains information about a password file used by the non-real-time kernel. However, Berg discloses wherein the integrity markers include a checksum and/or digital signature of a data element that maintains information about a password file used by the non-real-time kernel ([0027], lines 16-24 and [0072]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Sonic and Douglas as taught by Berg in order to ensure the confidentiality of sensitive information.

34. As to claim 29, neither Sonic nor Douglas explicitly discloses wherein the data element is an inode. However, Berg discloses wherein the data element is an inode ([0072]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Sonic and Douglas as taught by Berg in order to ensure the confidentiality of sensitive information.

35. As to claim 30, neither Sonic nor Douglas explicitly discloses wherein the application is programmed to encrypt and decrypt passwords stored in the password file. However, Berg discloses wherein the application is programmed to encrypt and decrypt passwords stored in the password file ([0027], lines 16-24 and [0072]).



Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Sonic and Douglas as taught by Berg in order to ensure the confidentiality of sensitive information.

36. Claims 32-35 and 37-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sonic and further in view of Douglas and O'Neal.

37. As to claim 32, Sonic discloses the real-time kernel (page 1). Neither Sonic nor Douglas explicitly discloses a challenge handler executing under the real-time kernel. However, O'Neal discloses a challenge handler executing under the real-time kernel (column 19, lines 10-20).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Sonic and Douglas as taught by O'Neal in order to in order to protect resources and to ensure safe and secure operations.

38. As to claim 33, Sonic doesn't explicitly disclose comprising an external monitor. However, Douglas discloses an external monitor (column 2, lines 35-60 and column 9, lines 2-10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Sonic by including an external

monitor as taught by Douglas in order to provide notification of the intrusion or intrusion attempts.

39. As to claim 34, neither Sonic nor Douglas explicitly discloses wherein the challenge handler is responsive to challenges sent from the external monitor to the challenge handler. However, O'Neal discloses wherein the challenge handler is responsive to challenges sent from the external monitor to the challenge handler (column 19, lines 10-20).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Sonic and Douglas as taught by O'Neal in order to in order to protect resources and to ensure safe and secure operations.

40. As to claim 35, neither Sonic nor Douglas explicitly discloses wherein the challenge handler is configured to send a response to the external monitor in response to receiving from the external monitor a challenge. However, O'Neal discloses wherein the challenge handler is configured to send a response to the external monitor in response to receiving from the external monitor a challenge (column 19, lines 10-20).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Sonic and Douglas as taught by O'Neal in order to in order to protect resources and to ensure safe and secure operations.

41. As to claim 37, neither Sonic nor Douglas explicitly discloses wherein the external monitor is programmed to determine whether the response from the challenge handler was received by the external monitor within a predetermined amount of time. However, O'Neal discloses wherein the external monitor is programmed to determine whether the response from the challenge handler was received by the external monitor within a predetermined amount of time (column 19, lines 10-20).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Sonic and Douglas as taught by O'Neal in order to in order to protect resources and to ensure safe and secure operations.

42. As to claim 38, neither Sonic nor Douglas discloses wherein the external monitor is further programmed to raise an alarm if it determines that the response from the challenge handler was not received by the external monitor within the predetermined amount of time. However, O'Neal discloses wherein the external monitor is further programmed to raise an alarm if it determines that the response from the challenge handler was not received by the external monitor within the predetermined amount of time (column 19, lines 10-20).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Sonic and Douglas as taught

by O'Neal in order to in order to protect resources and to ensure safe and secure operations.

43. Claims 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Douglas and further in view of O'Neal, Terry and Berg.

44. As to claim 15, neither Douglas and O'Neal nor Terry explicitly discloses wherein the security process is further configured to transmit the data item to the external monitor using an encryption key included in a challenge sent to the challenge handler. However, Berg discloses wherein the security process is further configured to transmit the data item to the external monitor using an encryption key included in a challenge sent to the challenge handler ([0007], [0027], lines 16-24 and [0072]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Douglas, O'Neal and Terry as taught by Berg in order to ensure the confidentiality of sensitive information.

45. As to claim 16, Douglas doesn't explicitly disclose wherein the security process is further configured to transmit the data item to the external monitor within a predetermined amount of time from when the external monitor sent a challenge to the challenge handler. However, O'Neal discloses wherein the security process is further configured to transmit the data item to the external monitor within a predetermined

amount of time from when the external monitor sent a challenge to the challenge handler (column 19, lines 10-20).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Douglas as taught by O'Neal in order to protect resources and to ensure safe and secure operations.

46. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sonic and further in view of Douglas, O'Neal and Berg.

47. As to claim 36, neither Sonic and Douglas nor O'Neal explicitly discloses wherein the response includes an encrypted data item. However, Berg discloses wherein the response includes an encrypted data item ([0007], which describes encrypting and decrypting communications).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Sonic, Douglas and O'Neal as taught by Berg in order to increase the security of transferred data.

48. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant.

Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the

responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

***Response to Amendment***

49. Applicant has amended claims 1-2, 4-7, 14-17 and 25-26. See rejection above.

***Response to Arguments***

50. Applicant's arguments filed on 13 September 2007 have been fully considered but they are not persuasive.

51. Regarding Applicant's remarks that "O'Neal doesn't disclose a deterministic network", it is the Examiner's position that O'Neal discloses deterministic network (O'Neal teaches deterministic network by setting a predetermined time to receive a response message; responds are sent within a predetermined amount of time which makes the network to be deterministic, - e.g. see -col. 19, lines 10-20).

52. Applicant argues that: "Applicant admits that O'Neal discloses a monitor that is configured such that if the monitor does not receive a response within a predetermined amount of time from sending a challenge, the monitor issues a notification. However, nowhere does O'Neal teach or suggest that the predetermined amount of time could be as little as 5 milliseconds."

Examiner has carefully reviewed Applicant's argument and maintains that: Claim 1 recites "a response to the challenge in less than about five millisecond from the challenge handler receiving the challenge". Applicant should note that the phrase "about" makes it indefinite to set an upper or lower boundary to how long a response should take. O'Neal discloses response takes predetermined amount of time (i.e. col. 19, lines 10-25). Applicant should note that "a predetermined amount of time" can be configured as any give time.

53. Applicant argues that: "claim 1 also requires "a real-time operating system." The Office contends that Douglas discloses a "real-time operating system." Applicant respectfully disagrees."

Examiner maintains that: Douglas discloses a "real-time operating system" (col. 2, lines 35-60, which describes file integrity checking feature for an additional level of detection. Applicant should note that Douglas has integrity checking feature which would require real time processing in order to maintain the integrity of applications. Douglas discloses HIDS sensor which runs real time which would require real time operating system, -e.g. see col. 9, lines 3-15).

54. Applicant argues that: "Even if we assume for the sake of argument that the Linux kernel is a thread running under a real-time kernel, Douglas would still not disclose the feature in question because the Linux kernel does not (a) monitor the integrity of an application running under the non-real-time kernel or (b) monitor integrity of a thread that is configured to monitor the integrity of an application running under the

non-real-time kernel. That is, neither the claimed "first thread" or claimed "second thread" reads on the Linux kernel disclosed in Douglas."

Examiner maintains that: Douglas discloses the first thread being configured to monitor the integrity of an application (col. 2, lines 45-50, "...integrity checking feature"); a second real-time thread running under the real-time kernel (col. 2, lines 35-60, which describes file integrity checking feature for an additional level of detection. Applicant should note that Douglas has integrity checking feature which would require real time processing in order to maintain the integrity of applications), the second real-time thread being configured to monitor integrity of the first real-time thread (col. 2, lines 35-60); and a security process running under the non-real-time kernel, the security process being configured to-check the integrity of the first real-time thread and/or the second real-time thread (column 9, lines 3-15, "The HIDS sensor 20 is capable of monitoring the integrity of the Linux kernel", see also column 4, lines 44-60, in which sensor reads as security process which being configured to check the integrity of threads that are running under Linux kernel).

55. Applicant argues in page 15 that: "Williams does not disclose a security process, let alone an integrity check performed by the security process that includes checking an executing schedule of the application."

Examiner maintains that: In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re*



*Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Furthermore, Douglas discloses a security process, let alone an integrity check performed by the security process (col. 9, lines 3-15, col. 2, lines 30-50). Williams discloses wherein a process includes checking an execution schedule of the application (abstract, column 4, lines 39-45 and column 6, lines 30-40).

56. In response to Applicant's argument that "Terry does not disclose checking the integrity of application code", it is the Examiner's position that Terry discloses checking the integrity of application code (Applicant should note that Terry teaches checking the integrity of application code by checking whether or not a registry for an application is modified or not, e.g. see -[0074]).

57. In response to applicant's argument in page 19 that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, In this case, motivation for the rejections is found both in the knowledge generally available to one of ordinary skill in the art and in the cited references.

***Conclusion***

58. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

59. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

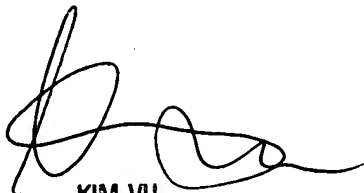
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

Application/Control Number:  
10/733,469  
Art Unit: 2135

Page 26

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100